

# Official Journal of the European Union

L 235



English edition

Legislation

Volume 58

9 September 2015

## Contents

### II *Non-legislative acts*

#### REGULATIONS

- ★ **Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market <sup>(1)</sup> ..... 1**
- ★ **Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market <sup>(1)</sup> ..... 7**
- Commission Implementing Regulation (EU) 2015/1503 of 8 September 2015 establishing the standard import values for determining the entry price of certain fruit and vegetables ..... 21

#### DECISIONS

- ★ **Commission Implementing Decision (EU) 2015/1504 of 7 September 2015 granting derogations to certain Member States as regards the provision of statistics pursuant to Regulation (EC) No 1099/2008 of the European Parliament and of the Council on energy statistics (notified under document C(2015) 6105) <sup>(1)</sup> ..... 24**
- ★ **Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market <sup>(1)</sup> ..... 26**

<sup>(1)</sup> Text with EEA relevance

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

- ★ Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market<sup>(1)</sup> ..... 37

---

<sup>(1)</sup> Text with EEA relevance

## II

*(Non-legislative acts)*

## REGULATIONS

## COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501

of 8 September 2015

**on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market**

*(Text with EEA relevance)*

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC <sup>(1)</sup>, and in particular Article 12(8) thereof,

Whereas:

- (1) Article 12(2) of Regulation (EU) No 910/2014 provides that an interoperability framework should be established for the purposes of interoperability of the national electronic identification schemes notified pursuant to Article 9(1) of that Regulation.
- (2) Nodes play a central role in the interconnection of Member States' electronic identification schemes. Their contribution is explained in the documentation related to the Connecting Europe Facility established by Regulation (EU) No 1316/2013 of the European Parliament and of the Council <sup>(2)</sup>, including the functions and components of the 'eIDAS node'.
- (3) Where a Member State or the Commission provides software to enable authentication to a node operated in another Member State, the party which supplies and updates the software used for the authentication mechanism may agree with the party which hosts the software how the operation for the authentication mechanism will be managed. Such an agreement should not impose disproportionate technical requirements or costs (including support, responsibilities, hosting and other costs) on the hosting party.
- (4) To the extent that the implementation of the interoperability framework justifies, further technical specifications providing details on technical requirements as set out in this Regulation could be developed by the Commission, in cooperation with Member States, in particular having regard to opinions of the Cooperation Network referred to in Article 14(d) of Commission Implementing Decision (EU) 2015/296 <sup>(3)</sup>. Such specifications should be developed as part of the digital service infrastructures of Regulation (EU) No 1316/2013 which provides the means for the practical implementation of an electronic identification building block.

<sup>(1)</sup> OJ L 257, 28.8.2014, p. 73.

<sup>(2)</sup> Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010 (OJ L 348, 20.12.2013, p. 129).

<sup>(3)</sup> Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 53, 25.2.2015, p. 14).

- (5) The technical requirements set out in this Regulation should be applicable despite any changes in the technical specifications that might be developed pursuant to Article 12 of this Regulation.
- (6) Large-scale pilot STORK, including specifications developed by it, and the principles and concepts of the European Interoperability Framework for European Public Services have been taken into the utmost account when establishing the arrangements of the interoperability framework set out in this Regulation.
- (7) The results of the cooperation between Member States have been taken into utmost account.
- (8) The measures provided for in this Regulation are in accordance with the opinion of the Committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

#### *Article 1*

#### **Subject matter**

This Regulation lays down technical and operational requirements of the interoperability framework in order to ensure the interoperability of the electronic identification schemes which Member States notify to the Commission.

Those requirements include in particular:

- (a) minimum technical requirements related to the assurance levels and the mapping of national assurance levels of notified electronic identification means issued under notified electronic identification schemes under Article 8 of Regulation (EU) No 910/2014 as set out in Articles 3 and 4;
- (b) minimum technical requirements for interoperability, as set out in Articles 5 and 8;
- (c) the minimum set of person identification data uniquely representing a natural or legal person as set out in Article 11 and in the Annex;
- (d) common operational security standards as set out in Articles 6, 7, 9 and 10;
- (e) arrangements for dispute resolution as set out in Article 13.

#### *Article 2*

#### **Definitions**

For the purposes of this Regulation, the following definitions shall apply:

- (1) 'node' means a connection point which is part of the electronic identification interoperability architecture and is involved in cross-border authentication of persons and which has the capability to recognise and process or forward transmissions to other nodes by enabling the national electronic identification infrastructure of one Member State to interface with national electronic identification infrastructures of other Member States;
- (2) 'node operator' means the entity responsible for ensuring that the node performs correctly and reliably its functions as a connection point.

*Article 3***Minimum technical requirements related to the assurance levels**

Minimum technical requirements related to the assurance levels shall be as set out in Commission Implementing Regulation (EU) 2015/1502 <sup>(1)</sup>.

*Article 4***Mapping of national assurance levels**

The mapping of national assurance levels of the notified electronic identification schemes shall follow the requirements laid down in Implementing Regulation (EU) 2015/1502. The results of the mapping shall be notified to the Commission using the notification template laid down in Commission Implementing Decision (EU) 2015/1505 <sup>(2)</sup>.

*Article 5***Nodes**

1. A node in one Member State shall be able to connect with nodes of other Member States.
2. The nodes shall be able to distinguish between public sector bodies and other relying parties through technical means.
3. A Member State implementation of the technical requirements set out in this Regulation shall not impose disproportionate technical requirements and costs on other Member States in order for them to interoperate with the implementation adopted by the first Member State.

*Article 6***Data privacy and confidentiality**

1. Protection of privacy and confidentiality of the data exchanged and the maintenance of data integrity between the nodes shall be ensured by using best available technical solutions and protection practices.
2. The nodes shall not store any personal data, except for the purpose set out in Article 9(3).

*Article 7***Data integrity and authenticity for the communication**

Communication between the nodes shall ensure data integrity and authenticity to make certain that all requests and responses are authentic and have not been tampered with. For this purpose, nodes shall use solutions which have been successfully employed in cross-border operational use.

<sup>(1)</sup> Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (see page 7 of this Official Journal).

<sup>(2)</sup> Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (see page 26 of this Official Journal)

*Article 8***Message format for the communication**

The nodes shall use for syntax common message formats based on standards that have already been deployed more than once between Member States and proven to work in an operational environment. The syntax shall allow:

- (a) proper processing of the minimum set of person identification data uniquely representing a natural or legal person;
- (b) proper processing of the assurance level of the electronic identification means;
- (c) distinction between public sector bodies and other relying parties;
- (d) flexibility to meet the needs of additional attributes relating to identification.

*Article 9***Management of security information and metadata**

1. The node operator shall communicate the metadata of the node management in a standardised machine processable manner and in a secure and trustworthy way.
2. At least the parameters relevant to security shall be retrieved automatically.
3. The node operator shall store data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be stored for a period of time in accordance with national requirements and, as a minimum, shall consist of the following elements:
  - (a) node's identification;
  - (b) message identification.
  - (c) message date and time.

*Article 10***Information assurance and security standards**

1. Node operators of nodes providing authentication shall prove that, in respect of the nodes participating in the interoperability framework, the node fulfils the requirements of standard ISO/IEC 27001 by certification, or by equivalent methods of assessment, or by complying with national legislation.
2. Node operators shall deploy security critical updates without undue delay.

*Article 11***Person identification data**

1. A minimum set of person identification data uniquely representing a natural or a legal person shall meet the requirements set out in the Annex when used in a cross-border context.
2. A minimum data set for a natural person representing a legal person shall contain the combination of the attributes listed in the Annex for natural persons and legal persons when used in a cross-border context.
3. Data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters.

*Article 12***Technical specifications**

1. Where it is justified by the process of implementation of the interoperability framework, the Cooperation Network established by Implementing Decision (EU) 2015/296 may adopt opinions pursuant to Article 14(d) thereof on the need to develop technical specifications. Such technical specifications shall provide further details on technical requirements as set out in this Regulation.
2. Pursuant to the opinion referred to in paragraph 1 the Commission in cooperation with Member States shall develop the technical specifications as part of the digital service infrastructures of Regulation (EU) No 1316/2013.
3. The Cooperation Network shall adopt an opinion pursuant to Article 14(d) of Implementing Decision (EU) 2015/296 in which it evaluates whether and to what extent the technical specifications developed under paragraph 2 correspond to the need identified in the opinion referred to in paragraph 1 or the requirements set in this Regulation. It may recommend that Member States take the technical specifications into account when implementing the interoperability framework.
4. The Commission shall provide a reference implementation as an example interpretation of the technical specifications. Member States may apply this reference implementation or use it as a sample when testing other implementations of the technical specifications.

*Article 13***Dispute resolution**

1. Where possible, any dispute concerning the interoperability framework shall be resolved by the concerned Member States through negotiation.
2. If no solution is reached in accordance with paragraph 1, the Cooperation Network established in accordance with Article 12 of Implementing Decision (EU) 2015/296 shall have competence in the dispute in accordance with its rules of procedure.

*Article 14***Entry into force**

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States

Done at Brussels, 8 September 2015.

*For the Commission*

*The President*

Jean-Claude JUNCKER

---

## ANNEX

**Requirements concerning the minimum set of person identification data uniquely representing a natural or a legal person, referred to in Article 11****1. The minimum data set for a natural person**

The minimum data set for a natural person shall contain all of the following mandatory attributes:

- (a) current family name(s);
- (b) current first name(s);
- (c) date of birth;
- (d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

The minimum data set for a natural person may contain one or more of the following additional attributes:

- (a) first name(s) and family name(s) at birth;
- (b) place of birth;
- (c) current address;
- (d) gender.

**2. The minimum data set for a legal person**

The minimum data set for a legal person shall contain all of the following mandatory attributes:

- (a) current legal name;
- (b) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

The minimum data set for a legal person may contain one or more of the following additional attributes:

- (a) current address;
- (b) VAT registration number;
- (c) tax reference number;
- (d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council <sup>(1)</sup>;
- (e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012 <sup>(2)</sup>;
- (f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013 <sup>(3)</sup>;
- (g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012 <sup>(4)</sup>.

---

<sup>(1)</sup> Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ L 258, 1.10.2009, p. 11).

<sup>(2)</sup> Commission Implementing Regulation (EU) No 1247/2012 of 19 December 2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories (OJ L 352, 21.12.2012, p. 20).

<sup>(3)</sup> Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights (OJ L 341, 18.12.2013, p. 10).

<sup>(4)</sup> Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004 (OJ L 121, 8.5.2012, p. 1).

**COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502****of 8 September 2015****on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market****(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC <sup>(1)</sup>, and in particular Article 8(3) thereof,

Whereas:

- (1) Article 8 of Regulation (EU) No 910/2014 provides that an electronic identification scheme notified pursuant to Article 9(1) needs to specify assurance levels low, substantial and high for electronic identification means issued under that scheme.
- (2) Determining the minimum technical specifications, standards and procedures is essential in order to ensure common understanding of the details of the assurance levels and to ensure interoperability when mapping the national assurance levels of notified electronic identification schemes against the assurance levels under Article 8 as provided by Article 12(4)(b) of Regulation (EU) No 910/2014.
- (3) International standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in this implementing act as being the principle international standard available in the domain of assurance levels for electronic identification means. However, the content of Regulation (EU) No 910/2014 differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account. Therefore the Annex, while building on this international standard should not make reference to any specific content of ISO/IEC 29115.
- (4) This Regulation has been developed as an outcome based approach as being the most appropriate which is also reflected in the definitions used to specify the terms and concepts. They take into account the aim of Regulation (EU) No 910/2014 in relation to assurance levels of the electronic identification means. Therefore, the Large-Scale Pilot STORK, including specifications developed by it, and the definitions and concepts in ISO/IEC 29115 should be taken into the utmost account when establishing the specifications and procedures set out in this implementing act.
- (5) Depending on the context in which an aspect of evidence of identity needs to be verified, authoritative sources can take many forms, such as registries, documents, bodies inter alia. Authoritative sources may be different in the various Member States even in a similar context.
- (6) Requirements for identity proofing and verification should take into account different systems and practices, while ensuring sufficiently high assurance in order to establish the necessary trust. Therefore, acceptance of procedures used previously for a purpose other than the issuance of electronic identification means should be made conditional upon confirmation that those procedures fulfil the requirements foreseen for the corresponding assurance level.

<sup>(1)</sup> OJ L 257, 28.8.2014, p. 73.

- (7) Certain authentication factors such as shared secrets, physical devices and physical attributes are usually employed. However, the usage of a greater number of authentication factors, especially from different factor categories, should be encouraged to increase the security of the authentication process.
- (8) This Regulation should not affect representation rights of legal persons. However, the Annex should provide for requirements for the binding between the electronic identification means of natural and legal persons.
- (9) The importance of information security and service management systems should be recognised, as should be the importance of employing recognised methodologies and applying the principles embedded in standards such as the ISO/IEC 27000 and the ISO/IEC 20000 series.
- (10) Good practices in relation to assurance levels in the Member States should also be taken into account.
- (11) IT security certification based on international standards is an important tool for verifying the security compliance of products with the requirements of this implementing act.
- (12) The Committee referred to in Article 48 of Regulation (EU) No 910/2014 has not delivered an opinion within the time limit laid down by its chair,

HAS ADOPTED THIS REGULATION:

#### *Article 1*

1. Assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme shall be determined with reference to the specifications and procedures set out in the Annex.
2. The specifications and procedures set out in the Annex shall be used to specify the assurance level of the electronic identification means issued under a notified electronic identification scheme by determining the reliability and quality of following elements:
  - (a) enrolment, as set out in section 2.1 of the Annex to this Regulation pursuant to Article 8(3)(a) of Regulation (EU) No 910/2014;
  - (b) electronic identification means management, as set out in section 2.2 of the Annex to this Regulation pursuant to Article 8(3)(b) and (f) of Regulation (EU) No 910/2014;
  - (c) authentication, as set out in section 2.3 of the Annex to this Regulation pursuant to Article 8(3)(c) of Regulation (EU) No 910/2014;
  - (d) management and organisation, as set out in section 2.4 of the Annex to this Regulation pursuant to Article 8(3)(d) and (e) of Regulation (EU) No 910/2014.
3. When the electronic identification means issued under a notified electronic identification scheme meets a requirement listed in a higher assurance level then it shall be presumed to fulfil the equivalent requirement of a lower assurance level.
4. Unless otherwise stated in the relevant part of the Annex, all elements listed in the Annex for a particular assurance level of the electronic identification means issued under a notified electronic identification scheme shall be met in order to match the claimed assurance level.

#### *Article 2*

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 8 September 2015.

*For the Commission*

*The President*

Jean-Claude JUNKER

---

## ANNEX

**Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme****1. Applicable definitions**

For the purposes of this Annex, the following definitions shall apply:

- (1) 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity;
- (2) 'authentication factor' means a factor confirmed as being bound to a person, which falls into any of the following categories:
  - (a) 'possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it;
  - (b) 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it;
  - (c) 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute;
- (3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity;
- (4) 'information security management system' means a set of processes and procedures designed to manage to acceptable levels risks related to information security.

**2. Technical specifications and procedures**

The elements of technical specifications and procedures outlined in this Annex shall be used to determine how the requirements and criteria of Article 8 of Regulation (EU) No 910/2014 shall be applied for electronic identification means issued under an electronic identification scheme.

**2.1. Enrolment****2.1.1. Application and registration**

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"><li>1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.</li><li>2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.</li><li>3. Collect the relevant identity data required for identity proofing and verification.</li></ol> |
| Substantial     | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                  |
| High            | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                  |

## 2.1.2. Identity proofing and verification (natural person)

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.</li> <li>2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.</li> <li>3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Substantial     | <p>Level low, plus one of the alternatives listed in points 1 to 4 has to be met:</p> <ol style="list-style-type: none"> <li>1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity<br/>and<br/>the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person<br/>and<br/>steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;<br/>or</li> <li>2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it<br/>and<br/>steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;<br/>or</li> <li>3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council <sup>(1)</sup> or by an equivalent body;<br/>or</li> <li>4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.</li> </ol> |

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High            | <p>Requirements of either point 1 or 2 have to be met:</p> <p>1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met:</p> <p>(a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;</p> <p>and</p> <p>the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;</p> <p>or</p> <p>(b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body</p> <p>and</p> <p>steps are taken to demonstrate that the results of the earlier procedures remain valid;</p> <p>or</p> <p>(c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body</p> <p>and</p> <p>steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.</p> <p>OR</p> <p>2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.</p> |

(<sup>1</sup>) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

### 2.1.3. Identity proofing and verification (legal person)

| Assurance level | Elements Needed                                                                                                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <p>1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made.</p> |

| Assurance level | Elements Needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <ol style="list-style-type: none"> <li>2. The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source, where the inclusion of a legal person in the authoritative source is voluntary and is regulated by an arrangement between the legal person and the authoritative source.</li> <li>3. The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Substantial     | <p>Level low, plus one of the alternatives listed in points 1 to 3 has to be met:</p> <ol style="list-style-type: none"> <li>1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable) its registration number<br/>and<br/>the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source, where the inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector<br/>and<br/>steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;<br/>or</li> <li>2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body;<br/>or</li> <li>3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.</li> </ol> |
| High            | <p>Level substantial, plus one of the alternatives listed in points 1 to 3 has to be met:</p> <ol style="list-style-type: none"> <li>1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context<br/>and<br/>the evidence is checked to determine that it is valid according to an authoritative source;<br/>or</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Assurance level | Elements Needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <p>2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body</p> <p>and</p> <p>steps are taken to demonstrate that the results of this previous procedure remain valid;</p> <p>or</p> <p>3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body</p> <p>and</p> <p>steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.</p> |

#### 2.1.4. Binding between the electronic identification means of natural and legal persons

Where applicable, for binding between the electronic identification means of a natural person and the electronic identification means of a legal person ('binding') the following conditions apply:

- (1) It shall be possible to suspend and/or revoke a binding. The life-cycle of a binding (e.g. activation, suspension, renewal, revocation) shall be administered according to nationally recognised procedures.
- (2) The natural person whose electronic identification means is bound to the electronic identification means of the legal person may delegate the exercise of the binding to another natural person on the basis of nationally recognised procedures. However, the delegating natural person shall remain accountable.
- (3) Binding shall be done in the following manner:

| Assurance level | Elements Needed                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above.</li> <li>2. The binding has been established on the basis of nationally recognised procedures.</li> <li>3. The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.</li> </ol> |
| Substantial     | <p>Point 3 of level low, plus:</p> <ol style="list-style-type: none"> <li>1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high.</li> </ol>                                                                                                                                                                                                                         |

| Assurance level | Elements Needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <ol style="list-style-type: none"> <li>2. The binding has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source.</li> <li>3. The binding has been verified on the basis of information from an authoritative source.</li> </ol>                                                                                                                                                                                      |
| High            | <p>Point 3 of level low and point 2 of level substantial, plus:</p> <ol style="list-style-type: none"> <li>1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high.</li> <li>2. The binding has been verified on the basis of a unique identifier representing the legal person used in the national context; and on the basis of information uniquely representing the natural person from an authoritative source.</li> </ol> |

## 2.2. *Electronic identification means management*

### 2.2.1. Electronic identification means characteristics and design

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. The electronic identification means utilises at least one authentication factor.</li> <li>2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.</li> </ol>                                          |
| Substantial     | <ol style="list-style-type: none"> <li>1. The electronic identification means utilises at least two authentication factors from different categories.</li> <li>2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.</li> </ol>                                          |
| High            | <p>Level substantial, plus:</p> <ol style="list-style-type: none"> <li>1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential</li> <li>2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.</li> </ol> |

### 2.2.2. Issuance, delivery and activation

| Assurance level | Elements needed                                                                                                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.                                              |
| Substantial     | After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs. |
| High            | The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.                                           |

## 2.2.3. Suspension, revocation and reactivation

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.</li> <li>2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.</li> <li>3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.</li> </ol> |
| Substantial     | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| High            | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                         |

## 2.2.4. Renewal and replacement

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level. |
| Substantial     | Same as level low.                                                                                                                                                                                                                                                                              |
| High            | <p>Level low, plus:</p> <p>Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.</p>                                                                                                                    |

## 2.3. Authentication

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls shall be understood to be commensurate to the risks at the given level.

## 2.3.1. Authentication mechanism

The following table sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.</li> <li>2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.</li> <li>3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.</li> </ol> |

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Substantial     | <p>Level low, plus:</p> <ol style="list-style-type: none"> <li>1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.</li> <li>2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.</li> </ol> |
| High            | <p>Level substantial, plus:</p> <p>The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.</p>                                                                                                                                                                                                                                |

#### 2.4. *Management and organisation*

All participants providing a service related to electronic identification in a cross-border context ('providers') shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.

##### 2.4.1. General provisions

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services.</li> <li>2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.</li> <li>3. Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services.</li> <li>4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.</li> <li>5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.</li> </ol> |
| Substantial     | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| High            | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## 2.4.2. Published notices and user information

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.</li> <li>2. Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.</li> <li>3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.</li> </ol> |
| Substantial     | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| High            | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## 2.4.3. Information security management

| Assurance level | Elements needed                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | There is an effective information security management system for the management and control of information security risks.                                                        |
| Substantial     | <p>Level low, plus:</p> <p>The information security management system adheres to proven standards or principles for the management and control of information security risks.</p> |
| High            | Same as level substantial.                                                                                                                                                        |

## 2.4.4. Record keeping

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.</li> <li>2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.</li> </ol> |
| Substantial     | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| High            | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## 2.4.5. Facilities and staff

The following table represents the requirements with respect to facilities and staff and subcontractors, if applicable, who undertake duties covered by this Regulation. Compliance with each of the requirements shall be proportionate to the level of risk associated with the assurance level provided.

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.</li> <li>2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.</li> <li>3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.</li> <li>4. Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.</li> </ol> |
| Substantial     | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| High            | Same as level low.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

#### 2.4.6. Technical controls

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | <ol style="list-style-type: none"> <li>1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.</li> <li>2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.</li> <li>3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.</li> <li>4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.</li> <li>5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.</li> </ol> |
| Substantial     | <p>Same as level low, plus:</p> <p>Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| High            | Same as level substantial.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

#### 2.4.7. Compliance and audit

| Assurance level | Elements needed                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low             | The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy. |

| Assurance level | Elements needed                                                                                                                                                                                                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Substantial     | The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.                                                                                                                                                               |
| High            | <ol style="list-style-type: none"><li>1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.</li><li>2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.</li></ol> |

**COMMISSION IMPLEMENTING REGULATION (EU) 2015/1503****of 8 September 2015****establishing the standard import values for determining the entry price of certain fruit and vegetables**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 1308/2013 of the European Parliament and of the Council of 17 December 2013 establishing a common organisation of the markets in agricultural products and repealing Council Regulations (EEC) No 922/72, (EEC) No 234/79, (EC) No 1037/2001 and (EC) No 1234/2007 <sup>(1)</sup>,

Having regard to Commission Implementing Regulation (EU) No 543/2011 of 7 June 2011 laying down detailed rules for the application of Council Regulation (EC) No 1234/2007 in respect of the fruit and vegetables and processed fruit and vegetables sectors <sup>(2)</sup>, and in particular Article 136(1) thereof,

Whereas:

- (1) Implementing Regulation (EU) No 543/2011 lays down, pursuant to the outcome of the Uruguay Round multilateral trade negotiations, the criteria whereby the Commission fixes the standard values for imports from third countries, in respect of the products and periods stipulated in Annex XVI, Part A thereto.
- (2) The standard import value is calculated each working day, in accordance with Article 136(1) of Implementing Regulation (EU) No 543/2011, taking into account variable daily data. Therefore this Regulation should enter into force on the day of its publication in the *Official Journal of the European Union*,

HAS ADOPTED THIS REGULATION:

*Article 1*

The standard import values referred to in Article 136 of Implementing Regulation (EU) No 543/2011 are fixed in the Annex to this Regulation.

*Article 2*

This Regulation shall enter into force on the day of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 8 September 2015.

*For the Commission,  
On behalf of the President,*

Jerzy PLEWA  
*Director-General for Agriculture and Rural Development*

---

<sup>(1)</sup> OJ L 347, 20.12.2013, p. 671.

<sup>(2)</sup> OJ L 157, 15.6.2011, p. 1.

## ANNEX

## Standard import values for determining the entry price of certain fruit and vegetables

| (EUR/100 kg)           |                        |                       |
|------------------------|------------------------|-----------------------|
| CN code                | Third country code (1) | Standard import value |
| 0702 00 00             | MA                     | 173,3                 |
|                        | MK                     | 48,7                  |
|                        | XS                     | 41,5                  |
|                        | ZZ                     | 87,8                  |
| 0707 00 05             | MK                     | 76,3                  |
|                        | TR                     | 116,3                 |
|                        | XS                     | 42,0                  |
|                        | ZZ                     | 78,2                  |
| 0709 93 10             | TR                     | 133,1                 |
|                        | ZZ                     | 133,1                 |
| 0805 50 10             | AR                     | 135,9                 |
|                        | BO                     | 135,7                 |
|                        | CL                     | 125,5                 |
|                        | UY                     | 142,2                 |
|                        | ZA                     | 136,9                 |
|                        | ZZ                     | 135,2                 |
| 0806 10 10             | EG                     | 239,8                 |
|                        | MK                     | 63,9                  |
|                        | TR                     | 129,5                 |
|                        | ZZ                     | 144,4                 |
| 0808 10 80             | AR                     | 188,7                 |
|                        | BR                     | 93,9                  |
|                        | CL                     | 134,4                 |
|                        | NZ                     | 143,4                 |
|                        | US                     | 112,5                 |
|                        | UY                     | 110,5                 |
|                        | ZA                     | 117,6                 |
|                        | ZZ                     | 128,7                 |
| 0808 30 90             | AR                     | 131,9                 |
|                        | CL                     | 100,0                 |
|                        | TR                     | 122,9                 |
|                        | ZA                     | 113,5                 |
|                        | ZZ                     | 117,1                 |
| 0809 30 10, 0809 30 90 | MK                     | 80,1                  |
|                        | TR                     | 141,7                 |
|                        | ZZ                     | 110,9                 |

| (EUR/100 kg) |                                   |                       |
|--------------|-----------------------------------|-----------------------|
| CN code      | Third country code <sup>(1)</sup> | Standard import value |
| 0809 40 05   | BA                                | 54,8                  |
|              | IL                                | 336,8                 |
|              | MK                                | 44,1                  |
|              | XS                                | 70,3                  |
|              | ZZ                                | 126,5                 |

<sup>(1)</sup> Nomenclature of countries laid down by Commission Regulation (EU) No 1106/2012 of 27 November 2012 implementing Regulation (EC) No 471/2009 of the European Parliament and of the Council on Community statistics relating to external trade with non-member countries, as regards the update of the nomenclature of countries and territories (OJ L 328, 28.11.2012, p. 7). Code 'ZZ' stands for 'of other origin'.

# DECISIONS

## COMMISSION IMPLEMENTING DECISION (EU) 2015/1504

of 7 September 2015

**granting derogations to certain Member States as regards the provision of statistics pursuant to Regulation (EC) No 1099/2008 of the European Parliament and of the Council on energy statistics**

*(notified under document C(2015) 6105)*

**(Only the Dutch, Estonian, French, Greek and Slovak texts are authentic)**

**(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EC) No 1099/2008 of the European Parliament and of the Council of 22 October 2008 on energy statistics <sup>(1)</sup>, and in particular Articles 5(4) and 10(2) thereof,

Whereas:

- (1) In accordance with Article 5(4) of Regulation (EC) No 1099/2008, at the duly justified request of a Member State, derogations may be granted for those parts of the national statistics for which the collection would lead to an excessive burden on respondents.
- (2) Requests have been submitted by Belgium, Estonia, Cyprus and Slovakia for obtaining derogations as regards the provision of statistics concerning the detailed energy consumption in households by type of end-use for certain reference years.
- (3) The information provided by those Member States justifies that derogations should be granted.
- (4) The measures provided for in this Decision are in accordance with the opinion of the European Statistical System Committee,

HAS ADOPTED THIS DECISION:

### Article 1

The following derogations from the provisions of Regulation (EC) No 1099/2008 shall be granted:

- (1) Belgium shall be granted a derogation from producing results for reference year 2015 for point 1.2.3 items 4.2.1 to 4.2.5, point 2.2.3 items 4.2.1 to 4.2.5, point 3.2.3 items 3.1 to 3.6, point 4.2.3 items 7.2.1 to 7.2.5 and point 5.2.4 items 4.2.1 to 4.2.5 of Annex B on statistics concerning the detailed energy consumption in households by type of end-use (as defined in point 2.3 item 26 'Other sectors — residential' of Annex A).

<sup>(1)</sup> OJ L 304, 14.11.2008, p. 1.

- (2) Estonia shall be granted a derogation from producing results for reference years 2015, 2016 and 2017 for point 1.2.3 items 4.2.1 to 4.2.5, point 2.2.3 items 4.2.1 to 4.2.5, point 3.2.3 items 3.1 to 3.6, point 4.2.3 items 7.2.1 to 7.2.5 and point 5.2.4 items 4.2.1 to 4.2.5 of Annex B on statistics concerning the detailed energy consumption in households by type of end-use (as defined in point 2.3 item 26 'Other sectors — residential' of Annex A).
- (3) Cyprus shall be granted a derogation from producing results for reference years 2015, 2016 and 2017 for point 1.2.3 items 4.2.1 to 4.2.5, point 2.2.3 items 4.2.1 to 4.2.5, point 3.2.3 items 3.1 to 3.6 and point 5.2.4 items 4.2.1 to 4.2.5 of Annex B on statistics concerning the detailed energy consumption in households by type of end-use (as defined in point 2.3 item 26 'Other sectors — residential' of Annex A).
- (4) Slovakia shall be granted a derogation from producing results for reference years 2015 and 2016 for point 1.2.3 items 4.2.1 to 4.2.5, point 2.2.3 items 4.2.1 to 4.2.5, point 3.2.3 items 3.1 to 3.6, point 4.2.3 items 7.2.1 to 7.2.5 and point 5.2.4 items 4.2.1 to 4.2.5 of Annex B on statistics concerning the detailed energy consumption in households by type of end-use (as defined in point 2.3 item 26 'Other sectors — residential' of Annex A).

#### *Article 2*

This Decision is addressed to the Kingdom of Belgium, the Republic of Estonia, the Republic of Cyprus and the Slovak Republic.

Done at Brussels, 7 September 2015.

*For the Commission*  
Marianne THYSSEN  
*Member of the Commission*

---

**COMMISSION IMPLEMENTING DECISION (EU) 2015/1505****of 8 September 2015****laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market****(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC <sup>(1)</sup>, and in particular Article 22(5) thereof,

Whereas:

- (1) Trusted lists are essential for the building of trust among market operators as they indicate the status of the service provider at the moment of supervision.
- (2) The cross-border use of electronic signatures has been facilitated through Commission Decision 2009/767/EC <sup>(2)</sup> which has set the obligation for Member States to establish, maintain and publish trusted lists including information related to certification service providers issuing qualified certificates to the public in accordance with Directive 1999/93/EC of the European Parliament and of the Council <sup>(3)</sup> and which are supervised and accredited by the Member States.
- (3) Article 22 of Regulation (EC) No 910/2014/EU provides the obligation for Member States to establish, maintain and publish trusted lists, in a secured manner, electronically signed or sealed in a form suitable for automated processing and to notify to the Commission the bodies responsible for establishing the national trusted lists.
- (4) A trust service provider and the trust services it provides should be considered qualified when the qualified status is associated to the provider in the trusted list. In order to ensure that other obligations stemming from Regulation (EU) No 910/2014, in particular those set in Articles 27 and 37, may be easily fulfilled by the service providers at a distance and by electronic means and in order to meet the legitimate expectations of other certification-service-providers who are not issuing qualified certificates but provide services related to electronic signatures under Directive 1999/93/EC and are listed by 30 June 2016, it should be possible for Member States to add trust services other than the qualified ones in the trusted lists, on a voluntary basis, at national level, provided that it is clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.
- (5) In line with recital 25 of Regulation (EU) No 910/2014, Member States may add other types of nationally defined trust services than those defined under Article 3(16) of Regulation (EU) No 910/2014, provided that it is clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.
- (6) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS DECISION:

*Article 1*

Member States shall establish, publish and maintain trusted lists including information on the qualified trust service providers which they supervise, as well as information on the qualified trust services provided by them. Those lists shall comply with the technical specifications set out in Annex I.

<sup>(1)</sup> OJ L 257, 28.8.2014, p. 73.

<sup>(2)</sup> Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 274, 20.10.2009, p. 36).

<sup>(3)</sup> Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

*Article 2*

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. The list shall clearly indicate which trust service providers and the trust services provided by them are not qualified.

*Article 3*

(1) Pursuant to Article 22(2) of Regulation (EU) No 910/2014, Member States shall sign or seal electronically the form suitable for automated processing of their trusted list in accordance with the technical specifications set out in Annex I.

(2) If a Member State publishes electronically a human readable form of the trusted list, it shall ensure that this form of the trusted list contains the same data as the form suitable for automated processing and it shall sign or seal it electronically in accordance with the technical specifications set out in Annex I.

*Article 4*

(1) Member States shall notify to the Commission the information referred to in Article 22(3) of Regulation (EU) No 910/2014 using the template in Annex II.

(2) The information referred to in paragraph 1 shall include two or more scheme operator public key certificates, with shifted validity periods of at least 3 months, which correspond to the private keys that can be used to sign or seal electronically the form suitable for automated processing of the trusted list and the human readable form when published.

(3) Pursuant to Article 22(4) of Regulation (EU) No 910/2014, the Commission shall make available to the public, through a secure channel to an authenticated web server, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed form suitable for automated processing.

(4) The Commission may make available to the public, through a secure channel to an authenticated web server, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed human readable form.

*Article 5*

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Decision shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 8 September 2015.

*For the Commission*

*The President*

Jean-Claude JUNCKER

---

## ANNEX I

## TECHNICAL SPECIFICATIONS FOR A COMMON TEMPLATE FOR TRUSTED LISTS

## CHAPTER I

## GENERAL REQUIREMENTS

The trusted lists shall include both current and all historical information, dating from the inclusion of a trust service provider in the Trusted Lists, about the status of listed trust services.

The terms 'approved', 'accredited' and/or 'supervised' in the present specifications also cover the national approval schemes but additional information on the nature of any such national schemes will be provided by Member States in their trusted list, including clarification on the possible differences with the supervision schemes applied to qualified trust service providers and the qualified trust services they provide.

The information provided in the trusted list is primarily aimed at supporting the validation of qualified trust service tokens, i.e. physical or binary (logical) objects generated or issued as a result of the use of a qualified trust service, e.g. namely qualified electronic signatures/seals, advanced electronic signatures/seals supported by a qualified certificate, qualified time-stamps, qualified electronic delivery evidences, etc.

## CHAPTER II

## DETAILED SPECIFICATIONS FOR THE COMMON TEMPLATE FOR THE TRUSTED LISTS

The present specifications rely on the specifications and requirements set in ETSI TS 119 612 v2.1.1 (here after referred to as ETSI TS 119 612).

When no specific requirement is set in the present specifications, requirements from ETSI TS 119 612 clauses 5 and 6 shall apply in their entirety. When specific requirements are set in the present specifications, they shall prevail over the corresponding requirements from ETSI TS 119 612. In case of discrepancies between the present specifications and specifications from ETSI TS 119 612, the present specifications shall prevail.

**Scheme name** (clause 5.3.6)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.6 where the following name shall be used for the scheme:

'EN\_name\_value' = 'Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.'

**Scheme information URI** (clause 5.3.7)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.7 where the 'appropriate information about the scheme' shall include as a minimum:

- (a) Introductory information common to all Member States with regard to the scope and context of the trusted list, the underlying supervision scheme and when applicable national approval (e.g. accreditation) scheme(s). The common text to be used is the text below, in which the character string '*(name of the relevant Member State)*' shall be replaced by the name of the relevant Member State:

'The present list is the trusted list including information related to the qualified trust service providers which are supervised by (*name of the relevant Member State*), together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.'

The cross-border use of electronic signatures has been facilitated through Commission Decision 2009/767/EC of 16 October 2009 which has set the obligation for Member States to establish, maintain and publish trusted lists with information related to certification service providers issuing qualified certificates to the public in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and which are supervised/accredited by the Member States. The present trusted list is the continuation of the trusted list established with Decision 2009/767/EC.'

Trusted lists are essential elements in building trust among electronic market operators by allowing users to determine the qualified status and the status history of trust service providers and their services.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

Member States may include in the trusted lists information on nationally defined trust services of other types than those defined under Article 3(16) of Regulation (EU) No 910/2014. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

(b) Specific information on the underlying supervision scheme and when applicable national approval (e.g. accreditation) scheme(s), in particular <sup>(1)</sup>:

- (1) Information on the national supervision system applicable to qualified and non-qualified trust service providers and the qualified and non-qualified trust services they provide as regulated by Regulation (EU) No 910/2014;
- (2) Information, where applicable, on the national voluntary accreditation schemes applicable to certification-service-providers having issued qualified certificates under Directive 1999/93/EC;

This specific information shall include, at least, for each underlying scheme listed above:

- (1) General description;
- (2) Information about the process followed for the national supervision system and, when applicable, for the approval under a national approval scheme.
- (3) Information about the criteria against which trust service providers are supervised or, where applicable, approved.
- (4) Information about the criteria and rules used to select supervisors/auditors and defining how they assess trust service providers and the trust services provided by them.
- (5) When applicable, other contact and general information that applies to the scheme operation.

#### **Scheme type/community/rules** (clause 5.3.9)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.9.

It shall only include UK English URIs.

<sup>(1)</sup> Those sets of information are of critical importance for relying parties to assess the quality and security level of such systems. Those sets of information shall be provided at Trusted List level through the use of the present 'Scheme information URI' (clause 5.3.7 — information being provided by Member State), 'Scheme type/community/rules' (clause 5.3.9 — through the use of a text common to all Member States) and 'TSL policy/legal notice' (clause 5.3.11 — a text common to all Member States, together with the ability for each Member State to add Member State specific text/references). Additional information on such systems for non-qualified trust services and nationally defined (qualified) trust services may be provided at service level when applicable and required (e.g. to distinguish between several quality/security levels) through the use of 'Scheme service definition URI' (clause 5.5.6).

It shall include at least two URIs:

- (1) A URI common to all Member States' Trusted Lists pointing towards a descriptive text that shall be applicable to all Trusted Lists, as follows:

URI: <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>

Descriptive text:

*Participation in a scheme*

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

*Policy/rules for the assessment of the listed services*

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

*Interpretation of the Trusted List*

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The "qualified" status of a trust service is indicated by the combination of the "Service type identifier" ("Sti") value in a service entry and the status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time". Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A "CA/QC" "Service type identifier" ("Sti") entry (possibly further qualified as being a "RootCA-QC" through the use of the appropriate "Service information extension" ("Sie") additionalServiceInformation Extension)

- indicates that any end-entity certificate issued by or under the CA represented by the "Service digital identifier" ("Sdi") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:
  - the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),
  - the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. “undersupervision”, “supervisionincessation”, “accredited” or “granted”) for that entry.

— **and IF** “Sie” “Qualifications Extension” information is present, then in addition to the above default rule, those certificates that are identified through the use of “Sie” “Qualifications Extension” information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the “SSCD support” and/or “Legal person as subject” (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific “Key usage” pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of “Qualifiers” used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

— to indicate the qualified certificate nature:

— “QCStatement” meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

— “QCForESig” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;

— “QCForESeal” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;

— “QCForWSA” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.

— to indicate that the certificate is not to be considered as qualified:

— “NotQualified” meaning the identified certificate(s) is(are) not to be considered as qualified; and/or

— to indicate the nature of the SSCD support:

— “QCWithSSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

— “QCNoSSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

— “QCSSCDStatusAsInCert” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

— to indicate the nature of the QSCD support:

— “QCWithQSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

— “QCNoQSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

— “QCQSCDStatusAsInCert” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

— “QCQSCDManagedOnBehalf” indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or

— to indicate issuance to Legal Person:

- “QCForLegalPerson” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

*Note:* The information provided in the trusted list is to be considered as accurate meaning that:

- if none of the id-etsi-qcs 1 statement, QCP OID or QCP + OID information is included in an end-entity certificate, and
- if no “Sie” “Qualifications Extension” information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a “QCStatement” qualifier, or
- an “Sie” “Qualifications Extension” information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a “NotQualified” qualifier,

then the certificate is not to be considered as qualified.

“Service digital identifiers” are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer’s or seal creator’s certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other “Sti” type entry is that, for that “Sti” identified service type, the listed service named according to the “Service name” field value and uniquely identified by the “Service digital identity” field value has the current qualified or approval status according to the “Service current status” field value as from the date indicated in the “Current status starting date and time”.

Specific interpretation rules for any additional information with regard to a listed service (e.g. “Service information extensions” field) may be found, when applicable, in the Member State specific URI as part of the present “Scheme type/community/rules” field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States’ trusted lists.’

- (2) A URI specific to each Member State’s trusted list pointing towards a descriptive text that shall be applicable to this Member State trusted list:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC> where CC = the ISO 3166-1 <sup>(1)</sup> alpha-2 Country Code used in the ‘Scheme territory’ field (clause 5.3.10)

- Where users can obtain the referenced Member State’s specific policy/rules against which trust services included in the list are assessed, in compliance with the Member State’s supervisory regime and where applicable, approval scheme.
- Where users can obtain a referenced Member State’s specific description about how to use and interpret the content of the trusted list with regard to the listed non-qualified trust services and/or to nationally defined trust services. This may be used to indicate a potential granularity in the national approval system related to CSPs not issuing QCs and how the ‘Scheme service definition URI’ (clause 5.5.6) and the ‘Service information extension’ field (clause 5.5.9) are used for this purpose.

Member States MAY define and use additional URIs expanding the above Member State specific URI (i.e. URIs defined from this hierarchical specific URI).

#### **TSL policy/legal notice** (clause 5.3.11)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.11 where the policy/legal notice concerning the legal status of the scheme or legal requirements met by the scheme under the jurisdiction in which it is established and/or any constraints and conditions under which the trusted list is maintained and published

<sup>(1)</sup> ISO 3166-1:2006: ‘Codes for the representation of names of countries and their subdivisions Part 1: Country codes’.

shall be a sequence of multilingual character strings (see clause 5.1.4) providing, in UK English as the mandatory language and optionally in one or more national languages, the actual text of any such policy or notice built as follows:

- (1) A first mandatory part, common to all Member States' Trusted Lists indicating the applicable legal framework, and whose English version is the following:

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Text in a Member State's national language(s):

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

- (2) A second, optional part, specific to each trusted list, indicating references to specific applicable national legal frameworks

#### **Service current status** (clause 5.5.4)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.5.4.

The migration of the 'Service current status' value of services listed in EUMS trusted list as of the day before the date Regulation (EU) No 910/2014 applies (i.e. 30 June 2016) shall be executed on the day the Regulation applies (i.e. 1 July 2016) as specified in Annex J to ETSI TS 119 612.

### CHAPTER III

#### **CONTINUITY OF TRUSTED LISTS**

Certificates to be notified to the Commission in accordance with Article 4(2) of this Decision shall meet the requirements of clause 5.7.1 from ETSI TS 119 612 and shall be issued in such a way that they:

- have at least a three months difference in their final date of validity ('Not After'),
- are created on new key pairs. Previously used key pairs must not be re-certified.

In case of expiry of one of the public key certificates that could be used to validate the trusted list's signature or seal that has been notified to the Commission and that is published in the Commission's central list of pointers, Member States shall:

- in case the currently published trusted list was signed or sealed with a private key whose public key certificate is expired, re-issue, without any delay, a new trusted list signed or sealed with a private key whose notified public key certificate is not expired;
- when required, generate new key pairs that could be used to sign or seal the trusted list and undertake the generation of their corresponding public key certificates;
- promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign or seal the trusted list.

In case of a compromise or decommissioning of one of the private keys corresponding to one of the public key certificates that could be used to validate the trusted list's signature or seal, that has been notified to the Commission and that is published in the Commission's central list of pointers, Member States shall:

- re-issue, without any delay, a new trusted list signed or sealed with a non-compromised private key in cases where the published trusted list was signed or sealed with a compromised or decommissioned private key;

- when required, generate new key pairs that could be used to sign or seal the trusted list and undertake the generation of their corresponding public key certificates;
- promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign or seal the trusted list.

In case of compromise or decommissioning of all the private keys corresponding to the public key certificates that could be used to validate the trusted list's signature, that have been notified to the Commission and that are published in the Commission's central list of pointers, Member States shall:

- generate new key pairs that could be used to sign or seal the trusted list and undertake the generation of their corresponding public key certificates;
- re-issue, without any delay, a new trusted list signed or sealed with one of those new private keys and whose corresponding public key certificate is to be notified;
- promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign or seal the trusted list.

#### CHAPTER IV

##### SPECIFICATIONS FOR THE HUMAN READABLE FORM OF THE TRUSTED LIST

When a human readable form of the trusted list is established and published, it shall be provided in the form of a Portable Document Format (PDF) document according to ISO 32000 <sup>(1)</sup> that shall be formatted according to the profile PDF/A (ISO 19005 <sup>(2)</sup>).

The content of the PDF/A based human readable form of the trusted list shall comply with the following requirements:

- The structure of the human readable form shall reflect the logical model described in TS 119 612;
- Every present field shall be displayed and provide:
  - The title of the field (e.g. 'Service type identifier');
  - The value of the field (e.g. 'http://uri.etsi.org/TrstSvc/Svctype/CA/QC');
  - The meaning (description) of the value of the field, when applicable (e.g. 'A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.');
  - Multiple natural language versions as provided in the trusted list, when applicable.
- The following fields and corresponding values of the digital certificates <sup>(3)</sup>, if present in the 'Service digital identity' field shall, as a minimum, be displayed in the human readable form:
  - Version
  - Certificate serial number
  - Signature algorithm
  - Issuer — all relevant distinguished name fields
  - Validity period
  - Subject — all relevant distinguished name fields

<sup>(1)</sup> ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7

<sup>(2)</sup> ISO 19005-2:2011: Document management — Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2)

<sup>(3)</sup> Recommendation ITU-T X.509 | ISO/IEC 9594-8: Information technology — Open systems interconnection — The Directory: Public-key and attribute certificate frameworks (see <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>)

- Public key
  - Authority Key Identifier
  - Subject Key Identifier
  - Key Usage
  - Extended key usage
  - Certificate Policies — all policy identifiers and policy qualifiers
  - Policy mappings
  - Subject alternative name
  - Subject directory attributes
  - Basic constraints
  - Policy constraints
  - CRL Distribution Points <sup>(1)</sup>
  - Authority Information Access
  - Subject Information Access
  - Qualified Certificate Statements <sup>(2)</sup>
  - Hash algorithm
  - Hash value of certificate
  - The human readable form shall be easily printable
  - The human readable form shall be signed or sealed by the Scheme Operator according to PDF advanced signature specified in Articles 1 and 3 of the Commission Implementing Decision (EU) 2015/1505.
- 

---

<sup>(1)</sup> RFC 5280: internet X.509 PKI Certificate and CRL Profile

<sup>(2)</sup> RFC 3739: internet X.509 PKI: Qualified Certificates Profile

## ANNEX II

## TEMPLATE FOR MEMBER STATES' NOTIFICATIONS

The information to be notified by Member States under Article 4(1) of the present Decision shall contain the following data and any changes thereto:

- (1) Member State, using ISO 3166-1 <sup>(1)</sup> Alpha 2 codes with the following exceptions:
  - (a) The Country Code for United Kingdom shall be 'UK'.
  - (b) The Country Code for Greece shall be 'EL'.
- (2) The body/bodies responsible for the establishment, maintenance and publication of the form suitable for automated processing and the human readable form of the trusted lists:
  - (a) Scheme operator name: the provided information must be identical — case sensitive — to the 'Scheme operator name' value present in the trusted list in as many languages as used in the trusted list.
  - (b) Optional information for internal Commission use only in cases where the relevant body needs to be contacted (the information will not be published in the EC compiled list of trusted lists):
    - Address of the scheme operator;
    - Contact details of the responsible person(s) (name, phone, e-mail address).
- (3) The location where the form suitable for automated processing of the trusted list is published (*location where the current trusted list is published*).
- (4) The location, when applicable, where the human readable trusted list is published (*location where the current trusted list is published*). In case a human readable trusted list is no longer published, an indication thereof.
- (5) The public key certificates which correspond to the private keys that can be used to sign or seal electronically the form suitable for automated processing of the trusted list and human readable form of the trusted lists: those certificates shall be provided as Privacy Enhanced Mail Base64 encoded DER certificates. For a change notification, additional information in case a new certificate is to replace a specific certificate in the Commission's list and in case the notified certificate is to be added to the existing one(s) without any replacement.
- (6) Date of submission of the data notified in points (1) to (5).

Data notified according to points (1), (2) (a), (3), (4) and (5) shall be included in the EC compiled list of trusted lists in replacement of the previously notified information included in that compiled list.

---

<sup>(1)</sup> ISO 3166-1: 'Codes for the representation of names of countries and their subdivisions — Part 1: Country codes'.

**COMMISSION IMPLEMENTING DECISION (EU) 2015/1506****of 8 September 2015**

**laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market**

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC <sup>(1)</sup>, and in particular Article 27(5) and 37(5) thereof,

Whereas:

- (1) Member States need to put in place the necessary technical means allowing them to process electronically signed documents that are required when using an online service offered by, or on behalf of, a public sector body.
- (2) Regulation (EU) No 910/2014 obliges Member States requiring an advanced electronic signature or seal for the use of an online service offered by, or on behalf of, a public sector body, to recognise advanced electronic signatures and seals, advanced electronic signatures and seals based on a qualified certificate and qualified electronic signatures and seals in specific formats, or alternative formats validated pursuant to specific reference methods.
- (3) To define the specific formats and reference methods, existing practices, standards and Union legal acts should be taken into account.
- (4) Commission Implementing Decision 2014/148/EU <sup>(2)</sup> has defined a number of the most common advanced electronic signature formats to be supported technically by the Member States, where advanced electronic signatures are required for an online administrative procedure. Establishing the reference formats aims at facilitating the cross-border validation of electronic signatures and at improving the cross-border interoperability of electronic procedures.
- (5) The standards listed in the Annex to this Decision are the existing standards for formats of advanced electronic signatures. Due to the ongoing revision by the standardisation bodies of the long term archival forms of the referenced formats, standards detailing long-term archiving are excluded from the scope of this Decision. When the new version of the referenced standards is available, references to the standards and the clauses on long term archiving will be revised.
- (6) Advanced electronic signatures and advanced electronic seals are similar from the technical point of view. Therefore, the standards for formats of advanced electronic signatures should apply *mutatis mutandis* to formats for advanced electronic seals.
- (7) Where other electronic signature or seal formats than those commonly technically supported are used to sign or seal, validation means that allow the electronic signatures or seals to be verified across borders should be provided. In order to allow the receiving Member States to be able to rely on those validation tools of another Member State, it is necessary to provide easily accessible information on those validation tools by including the information in the electronic documents, in the electronic signatures or in the electronic document containers.

<sup>(1)</sup> OJ L 257, 28.8.2014, p. 73.

<sup>(2)</sup> Commission Implementing Decision 2014/148/EU of 17 March 2014 amending Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 80, 19.3.2014, p. 7).

- (8) Where electronic signature or seal validation possibilities suitable for automated processing are available in a Member State's public services, such validation possibilities should be made available and provided to the receiving Member State. Nonetheless, this Decision should not impede the application of Articles 27(1) and (2) and 37(1) and (2) of Regulation (EU) No 910/2014 when the automated processing of validation possibilities for alternative methods is not possible.
- (9) In order to provide for comparable requirements for validation and to increase trust in the validation possibilities provided by Member States for other electronic signature or seal formats than those commonly supported, the requirements set out in this Decision for the validation tools, draw from the requirements for the validation of qualified electronic signatures and seals referred to in Articles 32 and 40 of Regulation (EU) No 910/2014.
- (10) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS DECISION:

#### *Article 1*

Member States requiring an advanced electronic signature or an advanced electronic signature based on a qualified certificate as provided for in Article 27(1) and (2) of Regulation (EU) No 910/2014, shall recognise XML, CMS or PDF advanced electronic signature at conformance level B, T or LT level or using an associated signature container, where those signatures comply with the technical specifications listed in the Annex.

#### *Article 2*

1. Member States requiring an advanced electronic signature or an advanced electronic signature based on a qualified certificate as provided for in Article 27(1) and (2) of Regulation (EU) No 910/2014, shall recognise other formats of electronic signatures than those referred to in Article 1 of this Decision, provided that the Member State where the trust service provider used by the signatory is established offers other Member States signature validation possibilities, suitable, where possible, for automated processing.
2. The signature validation possibilities shall:
  - (a) allow other Member States to validate the received electronic signatures online, free of charge and in a way that is understandable for non-native speakers;
  - (b) be indicated in the signed document, in the electronic signature or in the electronic document container; and
  - (c) confirm the validity of an advanced electronic signature provided that:
    - (1) the certificate that supports the advanced electronic signature was valid at the time of signing, and when the advanced electronic signature is supported by a qualified certificate, the qualified certificate that supports the advanced electronic signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I of Regulation (EU) No 910/2014 and that it was issued by a qualified trust service provider;
    - (2) the signature validation data corresponds to the data provided to the relying party;
    - (3) the unique set of data representing the signatory is correctly provided to the relying party;
    - (4) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

- (5) when the advanced electronic signature is created by a qualified electronic signature creation device, the use of any such device is clearly indicated to the relying party;
- (6) the integrity of the signed data has not been compromised;
- (7) the requirements provided for in Article 26 of Regulation (EU) No 910/2014 were met at the time of signing;
- (8) the system used for validating the advanced electronic signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues.

#### *Article 3*

Member States requiring an advanced electronic seal or an advanced electronic seal based on a qualified certificate as provided for in Article 37(1) and (2) of Regulation (EU) No 910/2014, shall recognise XML, CMS or PDF advanced electronic seal at conformance level B, T or LT or using an associated seal container where those comply with the technical specifications listed in the Annex.

#### *Article 4*

1. Member States requiring an advanced electronic seal or an advanced electronic seal based on a qualified certificate as provided for in Article 37(1) and (2) of Regulation (EU) No 910/2014, shall recognise other formats of electronic seals than those referred to in Article 3 of this Decision, provided that the Member State where the trust service provider used by the creator of the seal is established offers other Member States seal validation possibilities, suitable, where possible, for automated processing.

2. The seal validation possibilities shall:

- (a) allow other Member States to validate the received electronic seals online, free of charge and in a way that is understandable for non-native speakers;
- (b) be indicated in the sealed document, in the electronic seal or in the electronic document container
- (c) confirm the validity of an advanced electronic seal provided that:
  - (1) the certificate that supports the advanced electronic seal was valid at the time of sealing, and when the advanced electronic seal is supported by a qualified certificate, the qualified certificate that supports the advanced electronic seal was, at the time of sealing, a qualified certificate for electronic seal complying with Annex III of Regulation (EU) No 910/2014 and that it was issued by a qualified trust service provider;
  - (2) the seal validation data corresponds to the data provided to the relying party;
  - (3) the unique set of data representing the creator of the seal is correctly provided to the relying party;
  - (4) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of sealing;
  - (5) when the advanced electronic seal is created by a qualified electronic seal creation device, the use of any such device is clearly indicated to the relying party;
  - (6) the integrity of the sealed data has not been compromised;
  - (7) the requirements provided for in Article 36 of Regulation (EU) No 910/2014 were met at the time of sealing;
  - (8) the system used for validating the advanced electronic seal provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues.

*Article 5*

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Decision shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 8 September 2015.

*For the Commission*

*The President*

Jean-Claude JUNKER

---

## ANNEX

**List of technical specifications for XML, CMS or PDF advanced electronic signatures and the associated signature container**

Advanced electronic signatures mentioned in Article 1 of the Decision must comply with one of the following ETSI technical specifications with the exception of clause 9 thereof:

|                        |                                        |
|------------------------|----------------------------------------|
| XAdES Baseline Profile | ETSI TS 103171 v.2.1.1. <sup>(1)</sup> |
| CAdES Baseline Profile | ETSI TS 103173 v.2.2.1. <sup>(2)</sup> |
| PAdES Baseline Profile | ETSI TS 103172 v.2.2.2. <sup>(3)</sup> |

<sup>(1)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103171/02.01.01\\_60/ts\\_103171v020101p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf)

<sup>(2)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103173/02.02.01\\_60/ts\\_103173v020201p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf)

<sup>(3)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103172/02.02.02\\_60/ts\\_103172v020202p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf)

Associated signature container mentioned in Article 1 of the Decision must comply with the following ETSI technical specifications:

|                                                 |                                       |
|-------------------------------------------------|---------------------------------------|
| Associated Signature Container Baseline Profile | ETSI TS 103174 v.2.2.1 <sup>(1)</sup> |
|-------------------------------------------------|---------------------------------------|

<sup>(1)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103174/02.02.01\\_60/ts\\_103174v020201p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf)

**List of technical specifications for XML, CMS or PDF advanced electronic seals and the associated seal container**

Advanced electronic seals mentioned in Article 3 of the Decision must comply with one of the following ETSI technical specifications, with the exception of clause 9 thereof:

|                        |                        |
|------------------------|------------------------|
| XAdES Baseline Profile | ETSI TS 103171 v.2.1.1 |
| CAdES Baseline Profile | ETSI TS 103173 v.2.2.1 |
| PAdES Baseline Profile | ETSI TS 103172 v.2.2.2 |

Associated seal container mentioned in Article 3 of the Decision must comply with the following ETSI technical specifications:

|                                            |                        |
|--------------------------------------------|------------------------|
| Associated Seal Container Baseline Profile | ETSI TS 103174 v.2.2.1 |
|--------------------------------------------|------------------------|









